UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

ORACLE USA., INC,)
a Colorado corporation,)
ORACLE AMERICA, INC.,)
a Delaware corporation; and)
ORACLE INTERNATIONAL)
CORPORATION,)
a California corporation,) Case No. 2:10-cv-0106-LRH-PAL
Plaintiffs,)
v.)
RIMINI STREET, INC.,)
a Nevada corporation; and)
SETH RAVIN, an individual,)
Defendants.)
)

AFFIDAVIT OF PAUL J. MATTAL

I, Paul J. Mattal, do hereby depose and state as follows:

1. Counsel for Oracle has asked me to testify about how typical computer systems handle file deletion and drive space reuse, and to describe typical configurations in which data in log files may be routinely discarded over time. I've also been asked to examine the Yahoo! Messenger instant messaging software for Windows, to explain the message archiving functions and settings in the software, and to describe the computer forensics implications of those settings for preserving Yahoo instant messages as evidence.
2. I am a computer scientist and computer forensics expert. I graduated from Princeton University with a bachelor's degree in Computer Science in the spring of 1997. I have been employed by Elysium Digital, L.L.C. ("Elysium"), a technology litigation consulting firm located in Cambridge, Massachusetts, since January of 1999. While at Elysium, I trained in computer forensics and founded Elysium's forensic practice. I have advised clients in more than one hundred matters and offered written and oral expert testimony in state, federal, and county courts.

3. Elysium provides services relating to information technology, computer forensics, and computer science for lawyers and parties to legal disputes. Our clients have included the United States Department of Justice and prominent law firms in Boston and across the United States. In addition, Elysium consultants serve as court-appointed experts to help courts address issues relating to electronic discovery, computer forensics, and computer science.

4. Elysium has extensive experience analyzing software, both generally and in the context of computer forensics, and has done so numerous times before. I have experience with a wide variety of operating systems and application software.

5. In most operating systems, when a file is stored on disk, the system reserves disk segments to store that file's data. The system tracks the segments allocated to each file, and does not store other files in already-used segments. When a file is deleted, the segments containing that file's data are usually returned to the unassigned segment pool, and the file can no longer be accessed, but the file's data stored in those segments remains intact. When another file on the disk is then created or modified, the system may assign it a segment previously assigned to the deleted file, and residual data from the deleted file may then be overwritten. On typical computers, the computer's operating system and applications regularly create and modify files, even without user intervention; each time this occurs, data from previously-deleted files may be destroyed.

6. Operating system and application software often stores logs of information or activities in files on disk. Typically, these programs discard old log entries after some period of time, or after certain size limits are exceeded, to avoid filling the disk with old logs. For example, most recent versions of the Windows operating system maintain system event logs, security logs, and application activity logs; in typical configurations, old entries in these log files are deleted when time or log size criteria are met. In UNIX and UNIX-like operating systems, tools like the logrotate program are often used to "rotate" logs, archiving or discarding previously-stored information once certain criteria have been met.

Accordingly, unless affirmative steps are taken to preserve these typically-overwritten entries, they will be lost.

7. Elysium has lab facilities to perform experiments using clean installations of Windows and application software. Using a clean installation of Windows XP in our lab, I downloaded Yahoo! Messenger software from the Yahoo website[1] and ran the installation program. As shown in Exhibit 1, The Help>About Yahoo! Messenger dialog box shows the version of the Yahoo! Messenger software I installed as "10.0.0.1270-us".

8. The Yahoo! Messenger software has an archive feature for recording messages sent or received. Choosing the Messenger>Preferences menu option and selecting the Archive tab, I was able to examine the default archive settings. As shown in Exhibit 2, the default setting is "Yes, save all of my messages, but clear them each time I sign out".

9. To confirm how the archive feature works, I performed an experiment. First, as shown in Exhibit 3, I opened the archive viewer to observe the archive to be empty. Then, as shown in Exhibit 4, I used Yahoo! Messenger to send myself a test message. As shown in Exhibit 5, upon opening the archive viewer again, the archive contained my test message. As shown in Exhibit 6, there also appeared a file in the archive directory on disk bearing a recent last-modification timestamp, suggesting this file contained my archived test message.

10. Next, I signed out of Yahoo! Messenger, and then signed back in. As shown in Exhibit 7, the archive viewer then showed no archived messages. As shown in Exhibit 8, the file that had appeared earlier in the archive directory was no longer present. As shown in Exhibit 9, there were also no files in the Windows Recycle Bin at the end of the experiment.

11. My experiments with Yahoo! Messenger demonstrate that, by default, Yahoo! Messenger saves an archive of messages sent or received by the software in files on disk, and deletes them when the

[1] http://messenger.yahoo.com

user signs off. At the moment of deletion, those message data are still present on the disk, but are thereafter at constant risk of being destroyed during the usual operation of the machine.

12. In typical computer systems, residual data from deleted files, like the log files Yahoo! Messenger archive files described above, are constantly being overwritten and destroyed during the usual operation of the machine. To preserve as much of this data as possible, the power to the machine should be disconnected and a bit-for-bit forensic image of the computer's hard drives should be made by a qualified computer forensics expert, using a process designed not to alter the disks as the forensic images are made. Generally speaking, the sooner such forensic images are made the greater the likelihood that particular deleted data will be present in the forensic images.

Signed under pains and penalties of perjury this 24 day of August, 2010.

Pal J

Paul J. Mattal